(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－215379
（P2000－215379A）
(43)公開日　平成12年８月４日(2000.8.4)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０８Ｃ　19/00		Ｇ０８Ｃ　19/00	Ａ	
Ｇ０９Ｃ　1/00	６３０	Ｇ０９Ｃ　1/00	６３０Ｃ	
	６４０		６４０Ｂ	
Ｈ０４Ｌ　9/08		Ｈ０４Ｎ　1/387		
Ｈ０４Ｎ　1/387		Ｈ０４Ｌ　9/00	６０１Ｃ	

審査請求　未請求　請求項の数13　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願平11－205709

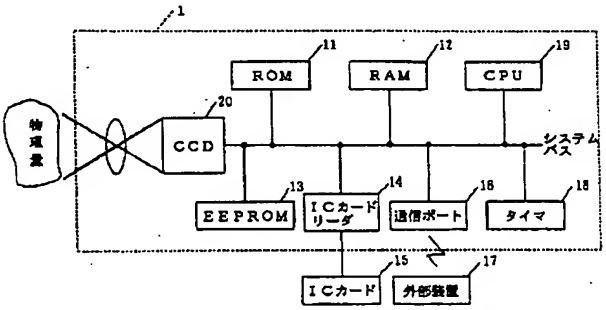
(22)出願日　平成11年７月21日(1999.7.21)

(31)優先権主張番号　特願平10－326215
(32)優先日　平成10年11月17日(1998.11.17)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　谷内田　益義
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100093920
弁理士　小島　俊郎

(54)【発明の名称】　デジタル計測機器及び画像計測機器

(57)【要約】
【課題】　本発明は、電子デジタルデータの内容の信頼性及び証明力を高められるデジタル計測機器及び画像計測機器を提供することを目的とする。
【解決手段】　物理的な計測対象を計測し、計測した物理量の計測データに対して公開鍵暗号方式の電子署名を付与して計測データを管理する、本発明に係るデジタル計測機器は、公開鍵暗号方式の電子署名に用いる、少なくとも一対の公開鍵と秘密鍵を鍵生成アルゴリズムによって生成する鍵生成手段を有する。



1

【特許請求の範囲】

【請求項１】　物理的な計測対象を計測し、計測した物理量の計測データに対して公開鍵暗号方式の電子署名を付与して計測データを管理するデジタル計測機器において、

公開鍵暗号方式の電子署名に用いる、少なくとも一対の公開鍵と秘密鍵を鍵生成アルゴリズムによって生成する鍵生成手段を有することを特徴とするデジタル計測機器。

【請求項２】　前記計測データに対して前記秘密鍵を用いて計算した電子署名を前記計測データと共に記録する請求項１記載のデジタル計測機器。

【請求項３】　前記秘密鍵により署名された、外部から書き替え不可能な公開鍵証明書を記憶する請求項１記載のデジタル計測機器。

【請求項４】　計測された順番を示す、外部からの書き替え不可能なシーケンス番号を収容し、該シーケンス番号を前記計測データと共に記録する請求項１記載のデジタル計測機器。

【請求項５】　少なくとも１つの外部認証コードを収容し、該外部認証コードに対する外部認証が成立したときに前記鍵生成アルゴリズム、前記電子署名及び前記シーケンス番号の更新を可能とする請求項１～４のいずれかに記載のデジタル計測機器。

【請求項６】　画像データに対して公開鍵暗号方式の電子署名を付与する画像計測機器において、

画像の特徴量を画像データフォーマットの画像付帯情報の一部として有し、画像計測機器の秘密鍵を用いて画像付帯情報から電子署名を計算し、計算した電子署名を画像付帯情報として画像データフォーマット中に格納することを特徴とする画像計測機器。

【請求項７】　電子署名を計算する際に画像付帯情報のいずれかの情報を使用したのかを画像付帯情報として画像データフォーマット中に格納しておく請求項６記載の画像計測機器。

【請求項８】　画像の特徴量を含む画像付帯情報について特徴量を計算し、計算した特徴量を画像付帯情報として格納すると共に、特徴量を元に画像計測機器の秘密鍵を用いて電子署名を計算し、計算した電子署名を画像付帯情報として画像データフォーマット中に格納する請求項６記載の画像計測機器。

【請求項９】　画像の特徴量を含む画像付帯情報について特徴量を計算し、計算した特徴量を画像付帯情報として格納すると共に、特徴量を元に画像計測機器の秘密鍵を用いて電子署名を計算し、計算した電子署名を画像付帯情報として画像データフォーマット中に格納し、また特徴量を元に画像計測機器に装着された外部記憶手段に格納された秘密鍵を用いて電子署名を計算し、当該電子署名も画像付帯情報として画像データフォーマット中に格納する請求項６記載の画像計測機器。

2

【請求項１０】　電子署名の計算に使用する特徴量を計算する際に使用する画像付帯情報は、画像データのシリアル番号を含む請求項６～９のいずれかに記載の画像計測機器。

【請求項１１】　電子署名の計算に使用する特徴量を計算する際に使用する画像付帯情報は、画像計測機器のシリアル番号を含む請求項６～９のいずれかに記載の画像計測機器。

【請求項１２】　電子署名の計算に使用する特徴量を計算する際に使用する画像付帯情報は、電子署名の計算に使用する秘密鍵の対となる公開鍵を含む請求項６～９のいずれかに記載の画像計測機器。

【請求項１３】　電子署名の計算に使用する特徴量を計算する際に使用する画像付帯情報は、電子署名の計算に使用する秘密鍵の対となる公開鍵を公開鍵証明書の形で含む請求項６～９のいずれかに記載の画像計測機器。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデジタル計測機器及び画像計測機器に関し、詳細にはデジタルカメラ、スキャナ、センサ、ＦＡＸ（モデム）などから得られた入力をデジタルデータに変換し、そのデジタルデータに対して管理や伝送等の処理を施す装置のデータセキュリティに関する。

【０００２】

【従来の技術】近年、情報の電子化が急速に進み、あらゆる情報が電子データとしてネットワークやポータブルメディアを介して相互にやり取りされるようになっており、その電子データのセキュリティを確保するために様々な技術が開発されている。一般に検討されている電子データのセキュリティ技術は、主にデータの秘匿技術やデータの改ざん検知技術、データへのアクセス権の管理（認証を含む）技術等、データの内容には着目せず、端なる塊として扱うセキュリティ技術が多い一方、その電子データの内容が元々正しいかどうかに関する技術開発はあまりなされていなかった。しかし、セキュリティを確保しようとしている元々のデータが不正なものであれば、そのデータのセキュリティを確保しても何の意味もなさない。元々のデータが最初から人為的な操作によって電子的に生成されたものであれば、そのデータの内容が正しいことを保証するには、従来の技術のように、そのデータを作成した作成者もしくはそのデータに関して責任をもっている者の電子署名を付加するなどの処理を施すことになる。

【０００３】そこで、従来例として、米国特許第５，４９９，２９４号明細書には、デジタルカメラにそのデジタルカメラ固有のプライベートキーを格納し、そのデジタルカメラで撮影された画像ファイルに対して当該プライベートキーを用いて電子署名を計算して画像ファイルとともに媒体に記録するという方法が開示されている。

詳細には、デジタルカメラに格納しているプライベートキーはデジタルカメラ内のＳｅｃｕｒｅ　ＰｒｏｃｅｓｓｏｒにＲＯＭ化して記録されており外部から読み出すことができないようになっている。また、そのプライベートキーに対応するパブリックキーをデジタルカメラの本体に刻印する。更に、デジタルカメラで撮影した画像の周辺部にそのパブリックキーや撮影状況を示すパラメータなどを印字し、その画像全体に対して電子署名を施すようにしている。そのため、そのデジタルカメラで撮影した画像は証明力が高められている。なお、デジタルカメラに対応するパブリックキーはデジタルカメラの製造メーカが広く公開することを前提としている。

【０００４】

【発明が解決しようとする課題】しかしながら、上記従来例によれば、撮影した画像ファイルと、それに対してデジタルカメラが計算した電子署名ファイルが別々であるために画像ファイルをパソコン等に移した際にそれらの関連付けがわからなくなる可能性がある。そのため、せっかく画像ファイルの証明力を高める処理を施したのにもかかわらず、電子署名ファイルがどれだかわからなくなり結局画像ファイルの真正性を検証することができなくなるという問題があった。

【０００５】また、プライベートキーとパブリックキーのペアをデジタルカメラの製造メーカが生成し、カメラの内部に記録するようにしているが、デジタルカメラ製造メーカがプライベートキーを知っていることは証明力を低下させることに繋がるという問題もあった。

【０００６】更に、デジタルカメラ内蔵のタイマの設定を製造時点において設定した後、変更できないようにしているが、タイマが徐々に狂ってしまうことは当然起こりうることであり、正しい時刻に設定し直せないのは問題であった。それに、タイマの電源であるリチウムイオン電池が切れてしまうと時刻そのものの記録ができなくなるのも問題であった。

【０００７】また、上記従来例ではデジタルカメラ個々に割り振ったパブリックキー全てを製造メータが広く公開することになっているが、デジタルカメラが非常に数多く製造される場合を考えると、その数の分だけパブリックキーを公開するというのは煩雑さが増して画像の真正性検証の際に膨大なパブリックキーリストの中から該当するパブリックキーを探し出さなければならないという問題があった。

【０００８】更に、デジタルカメラのような一般ユーザ向けのデジタル機器を想定しているために、誰がそのデータを記録したのか、などについて全く考慮されていないという問題があった。例えば、ＣＴ装置やデジタル内視鏡装置などの医療用計測装置の場合には特に誰がそのデータを計測（撮影）したのかが重要となることがあるからである。

【０００９】また、デジタルカメラのような一般ユーザ向けの比較的安価なライフサイクルの短いデジタル機器を想定しているため、装置内部の電子署名アルゴリズムの追加・入れ替えや鍵の更新に関しては考慮されておらず、新しい製品モデルにおいて新しいアルゴリズムを搭載するとしか述べられていない。しかし、例えばＣＴ装置のような高額なデジタル医療機器の場合には、そのライフサイクルも長く、装置の寿命より短い機関で暗号アルゴリズムの強度が相対的に弱くなってしまうという可能性があるという問題があった。

【００１０】本発明はこれらの問題点を解決するためのものであり、電子デジタルデータの内容の信頼性及び証明力を高められるデジタル計測機器及び画像計測機器を提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明は前記問題点を解決するために、物理的な計測対象を計測した物理量の計測データを管理するデジタル計測機器において、公開鍵暗号方式の電子署名に用いる少なくとも一対の公開鍵と秘密鍵を鍵生成アルゴリズムによって生成する鍵生成手段を有することに特徴がある。よって、生成した秘密鍵は製造メーカすら知り得ない。

【００１２】また、計測データに対して秘密鍵を用いて計算した電子署名を計測データと共に記録することや秘密鍵により署名された外部から書き替え不可能な公開鍵証明書を記憶することにより、秘密鍵を公開せずとも公開鍵証明書を作成する際に使用した秘密鍵に対応する公開鍵のみで良い。

【００１３】更に、計測された順番を示す、外部からの書き替え不可能なシーケンス番号を収容し、該シーケンス番号を計測データと共に記録することにより、計測データの前後関係が混乱しないようにすることができる。

【００１４】また、少なくとも１つの外部認証コードを収容し、該外部認証コードに対する外部認証が成立したときに鍵生成アルゴリズム、電子署名及びシーケンス番号の更新を可能とすることにより、計測したデータの証明力を長期間維持できる。

【００１５】更に、別の発明として、画像の特徴量を画像データフォーマットの付帯情報の一部として有し、画像付帯情報から画像計測機器の秘密鍵を用いて電子署名を計算し、画像付帯情報として画像データフォーマット中に追加格納することにより、画像計測機器より得られた画像に電子署名を埋め込むので画像計測機器で撮影した画像が改ざんされていないかどうか検証できるようになっているし、画像の特徴量を画像付帯情報として格納し、電子署名を計算する際にどの画像付帯情報を使用して署名を計算したのかを明確できる。そうすることで電子署名を格納したことによって画像データの、証拠写真と関わらない部分の付帯情報についても変更や追加ができるようになった。

【００１６】

5

【発明の実施の形態】公開鍵暗号方式の電子署名に用いる少なくとも一対の公開鍵と秘密鍵を鍵生成アルゴリズムによって生成する鍵生成手段を有する。

【００１７】

【実施例】以下、本発明の実施例を図面に基づいて説明する。はじめに、電子データの内容、特に物理量の計測データとは、具体例を挙げれば、デジタルカメラで撮影した画像データや医療で使用するＣＴ（Ｃｏｍｐｕｔｅｄ　Ｔｏｍｏｇｒａｐｈｙ）装置で計測、計算した再構成画像データなどが挙げられる。これらのデータのように、計測したデータからその計測装置特有の処理（デジタルカメラの場合には画像の圧縮処理や階調変換処理などＣＴ装置の場合にはＦＢＰ（Ｆｉｌｔｅｒｅｄ　Ｂａｃｋ　Ｐｒｏｊｅｃｔｉｏｎ）法による画像再構成処理など）を施した後のデータなど、計測した物理量と関連付けを保証する必要が生じる（そのデータを他人に渡ったり、見せたりする場合には保証する必要が生じるものと考えられる）電子データが対象となる。そして、デジタルカメラやＣＴ装置など、一般には計測装置と呼ばれないような装置であっても、以上のような背景から「デジタル計測機器」と呼ばれている。

【００１８】図１は本発明の第１の実施例に係るデジタル計測機器の構成を示すブロックである。なお、本実施例のデジタル計測機器としてデジタルカメラを例として以下説明するものとする。同図に示す本実施例は、電子署名用の暗号アルゴリズム（例えばＲＳＡとＭＤ５など）、及び外部認証に使用する暗号アルゴリズム（例えばＤＥＳ（Ｄａｔｅ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）。このＤＥＳは秘密鍵暗号方式の暗号アルゴリズムであるが外部認証に使用できればどのような方式の暗号アルゴリズムでも構わない）、画像データ圧縮アルゴリズム（例えばＪＰＲＧ）、乱数発生アルゴリズム、メイン制御プログラムを格納するＲＯＭ１１と、メイン制御プログラム、各種アルゴリズム、秘密鍵、シーケンス番号、外部認証鍵等が必要に応じてロードされるＲＡＭ１２と、公開鍵暗号方式の電子署名に使用する秘密鍵、公開鍵証明書（公証機関の署名と公開鍵）、シーケンス番号や外部認証鍵を格納するＥＥＰＲＯＭ１３と、撮影したデジタル撮影画像データにシーケンス番号、時刻、電子署名などを付加したデジタル画像情報を記録する、例えばメモリカード等のＩＣカード１５の当該情報を読み出し／書き込みを行うＩＣカードリーダ１４、外部装置１７との通信によるやり取りを行うための通信ポート１６と、時刻データを取得するタイマ１８と、各種の演算を行いかつ各構成要素を制御するＣＰＵ１９と、撮影した画像を電子データに変換するＣＣＤ２０とを含んで構成されている。

【００１９】次に、本実施例の動作について説明すると、シャッタボタンが押されると、ＣＰＵ１９はタイマ１８から時刻データを取得し、それをＲＡＭ１２に記憶

6

すると同時にＣＣＤ２０から撮影画像データを取得してＲＡＭ１２に格納する。そして、格納された画像データを圧縮する。また、ＥＥＰＲＯＭ１３からシーケンス番号を取り出すと同時にシーケンス番号に１加えたシーケンス番号をＥＥＰＲＯＭ１３に格納する。圧縮された画像データの先頭に先に取り出したシーケンス番号と、タイマ１８から取得した時刻データを付加する。そして、できあがった画像情報に対してその電子署名を先の画像情報に付加して、一つの塊としての撮影情報としてＩＣカード１５に格納する。秘密鍵、公開鍵証明書、シーケンス番号、時刻設定を変更する際に、予め行うべき外部認証処理は、外部認証に使用するアルゴリズムに例えばＤＥＳを使用する場合を例に取ると以下の手順で行う。

【００２０】先ず、内部で乱数を発生させ、その乱数を外部装置に送出する。外部装置から認証コードを受け取り、先に生成した乱数を外部認証鍵により暗号化したコードと比較する。それらのコードが一致すれば外部認証が成立したこととし、セキュリティステータス（これはＲＡＭで管理しているフラグ。初期状態はＦＡＬＳＥとする）をＴＲＵＥに変更する。外部から秘密鍵、公開鍵証明書、シーケンス番号、時刻設定の変更を要求された場合には、先ず内部で管理しているセキュリティステータスを参照し、それがＦＡＬＳＥとなっている場合には要求を受け付けない。一方ＴＵＲＥとなっている場合には要求を受け付け、その要求に応じた処理を行う。処理を行うとセキュリティステータスをＦＡＬＳＥに変更する。

【００２１】次に、本実施例における計測データに対する処理の流れについて以下に説明する。先ず、既に装置のキーペア（このキーペアはプライベートキーとパブリックキーのペアのことである）が生成されているかどうかを調べ（ステップＳ１０１）、されていない場合は処理を終了するが、生成されていれば図１のＩＣカード１５からユーザ公開鍵証明書を取得する（ステップＳ１０２）。ＣＣＤ２０から計測データ（撮影データ）を取得し、更にタイマ１８から現在時刻を取得する（ステップＳ１０３，Ｓ１０４）。そして、取得した計測データに必要な処理、例えば圧縮、ＣＴ画像再構成、標準データフォーマットへの変換などを施し、処理済みの計測データを取得する（ステップＳ１０５）。次に、ＥＥＰＲＯＭ１３からプライベートキー・公開鍵証明書・シーケンス番号を取得する（ステップＳ１０６）。取得したシーケンス番号に１増加させてＥＥＰＲＯＭ１３に格納する（ステップＳ１０７）。処理済みの計測データに現在時刻及びシーケンス番号を追加されてたものを計測情報とする（ステップＳ１０８）。この計測情報に対してハッシュ値を計算する（ステップＳ１０９）。計算したハッシュ値はプライベートキーにより暗号化され、装置の電子署名を計算する（ステップＳ１１０）。上記計算されたハッシュ値をＩＣカードに渡し、ユーザのプライベー

トキーにより暗号化したユーザ電子署名を取得する（ステップＳ１１１）。そして、計測情報に装置の電子署名及び公開鍵証明書を追加し、装置の署名済みの計測情報とする（ステップＳ１１２）。更に、ユーザ電子署名やユーザ公開鍵証明書を追加して装置・ユーザの署名済み計測情報とする（ステップＳ１１３）。出来上がった署名済み計測情報をファイルとして大容量外部記録媒体に記録する（又は通信ポート１６から外部装置に送出する）（ステップＳ１１４）。

【００２２】このように、暗号処理機能及び記憶機能を持つＩＣカード等の外部記憶手段を使用してユーザの署名を生成し、ユーザの公開鍵証明書と共に装置の署名済計測情報に付与しているだけで計測装置自身はユーザの認証を行っていない。これは署名済み計測情報を検証すればユーザが誰であったか「後で」認証するができるためある。一方、計測装置自身が予めユーザを認証できれば他の方法であっても構わなく、計測装置にとってユーザが認証されてさえいれば単にユーザ名をシーケンス番号などと共に処理済み計測データに付与して電子署名処理を施しても構わない。ＩＣカードを使用しない場合には計測装置がＩＣカードリーダ１４を搭載する必要はない。装置の公開鍵証明書には装置のシリアル番号、製造メータ名などが記載されており、ユーザの公開鍵証明書にはユーザを特定できるユーザ名や所属などが記載されていることを想定している。装置の公開鍵証明書については外部からの要求に応じて装置が外部に送出することを可能とする。また、本実施例では、計測情報を作成してからすぐに電子署名の作成を行っているが電子署名の作成には計算時間がかかるため、連続して計測を行いたい場合には不都合が生じる可能性がある。そこで、作成した計測情報はそのまま大容量外部記憶媒体に記録しておき、後で外部に送出する前、又は大容量記憶媒体を計測情報から取り外す前に電子署名を作成・付与するようにしても良い。その場合には、電子署名を付与するまでは大容量外部記憶媒体が計測装置本体から取り外せないようにするなど電子署名を付与していない計測情報に外部装置からアクセスできないようにする必要がある。

【００２３】また、単に付帯情報（現在時刻、シーケンス番号、公開鍵証明書など）を処理済み計測データの後ろに追加するようにしているが、例えばＪＰＥＧ画像の場合には画像データフォーマットとして任意のデータを埋め込むことができるため、それを利用してその部分にそれら付帯情報を記録することもできる。そうすることで、電子署名が埋め込まれたファイルでありながら、既存の画像表示プログラムなどが処理することも可能となる。その際注意しなければならないのは、ＴＩＦＦなどの場合には画像データがどこからはじまっているのか、その絶対位置をタグとして持っているため、電子署名を埋め込んだ場合にはその絶対位置がずれてしまうことになる。そこで、そのような問題を回避するために、図３に示すように、予め電子署名を埋め込む分だけ領域を確保し、その領域は予め決められた値で埋めておき、その上でデータ全体に対してハッシュ値を計算し、電子署名を生成する。そして、生成された電子署名を予め確保しておいた領域に埋め込むということも可能である。データ計測を行う前に予めキーペア生成処理を実行していなければならない。この処理は例えば計測装置製造メーカが工場において出荷前に実行する。

【００２４】次に、キーペア生成処理について図４及び図５に基づいて説明すると、既にキーペアが計測機器のＥＥＰＲＯＭに記録されているかどうかを調べ（ステップＳ２０１）、キーペアが記録されていれば生成する必要がないので処理を終了する。一方、キーペアが記録されていないならば、図４に示すように、鍵生成アルゴリズムによりキーペアを生成する（ステップＳ２０２）。そして、生成したキーペアはＥＥＰＲＯＭに記録される（ステップＳ２０３）。次に、キーペアのうちパブリックキーは通信ポートを介して外部装置に送信される（ステップＳ２０４）。図４に示すように、外部装置においてパブリックキーに対して公開鍵証明書を作成され、当該公開鍵証明書は通信ポートを介してデジタル計測機器に渡される（ステップＳ２０５，Ｓ２０６）。そして、公開鍵証明書はＥＥＰＲＯＭに記録される（ステップＳ２０７）。

【００２５】また、計測装置の内部タイマを設定する処理は簡単な例で言えば計測装置にキーパッドを取付け、キーパッドからパスワードを入力し、計測装置が内部に保持しているパスワードと照合して正しければタイマの設定変更を許可するといった方法が考えられる。他にも上記本実施例のように計測装置がＩＣカードリーダを搭載しているので、特定のＩＣカードが挿入去れている場合にのみタイマの設定を変更できるようにすることも考えられる。挿入されているのが特定のＩＣカードかどうかを検証するためには例えば以下のような方法をとることができる。図６に示すように予め計測機器メーカのパブリックキーを計測装置内部に格納しておく。そして、計測装置が最初に生成した乱数と、ＩＣカードからの認証コードを復号した乱数’が一致すればＩＣカードは秘密の鍵を持っていることになり、特定のコードであることが認証できる。

【００２６】暗号アルゴリズムの更新処理については、例えばタイマの設定処理で説明すると、特定のＩＣカードを挿入している最中にのみ通信ポートを介して新しい暗号処理プログラムを受け取ることができるようにするようなことが考えられる。又は図７に示すように、暗号処理プログラムに製造メーカの電子署名を付与して計測装置に渡すと、計測装置がその電子署名を検証し、正しい電子署名であることが検証できれば、その暗号処理プログラムを内部記憶媒体に格納して暗号処理に使用する方法も考えられる。この例においても計測装置には予め

製造メーカの公開鍵を保持していることを想定している。暗号処理プログラムには、ハッシュ値を計算するアルゴリズムやキーペアを生成するアルゴリズム、そして暗号化するアルゴリズムや復号するアルゴリズムが含まれていることを想定している。

【００２７】また上記では暗号アルゴリズムの更新処理として述べたが、暗号アルゴリズムについては更新するのではなく、単に追加しかできないようにしても良い。後から登録する暗号アルゴリズムは当然のことながら強度が高いものを使用するべきであるが、古い暗号処理プログラムを持ってきて誰かが不正に計測装置にインストールした場合に、既に最新の暗号処理プログラムを搭載している計測装置の証明力が低下することを防ぐことができる。それだけでなく、古いアルゴリズムに比べ、最新の暗号アルゴリズムには欠陥が見つかる可能性が大きい。そのため、計測情報には古いアルゴリズムの電子署名と、新たにインストールした暗号アルゴリズムによる電子署名を両方付与するようにしても良い。また、暗号アルゴリズムについては、新しいアルゴリズムはより計算量を必要とする可能性が大きいため、暗号処理プログラムとしての入れ替えでなく、暗号処理プログラムを実行するプロセッサの入れ替えを行うようにしても良い。その場合、暗号処理プロセッサが正当な製造メーカにより作られたものかどうか認証する必要があるが、その仕組みは先に特定のＩＣカードかどうかを検証する処理と全く同じ処理を適用することができる。暗号処理プロセッサモジュールは例えばＰＣＭＣＩＡカードなどのような形態が考えられる。又は、暗号処理プロセッサと計測装置との間の物理的なインタフェースを特殊なものにしたり、計測装置のプロセッサと暗号処理プロセッサとの間のプロトコルを特殊なものにして非公開にするなどの方法を取っても良い。そのような場合には暗号処理プロセッサを認証する必要はない。計測装置のプロセッサと暗号処理のためのプロセッサに分けた場合の計測装置の構成は図８のようになるが詳細な説明は省略する。

【００２８】上記第１の実施例では、計測データの中に電子署名を格納するフィールドを予約し、その部分を予めＮＵＬＬパディングした状態の計測データ全体に対してデジタル計測機器が電子署名を計算し、その電子署名を先の予約フィールドに格納する方法をとっていた。この方法の場合、計測データに電子署名を格納した後で、さらに計測データの中に他の情報、例えばコメントなどを格納したくなった場合に問題があった。つまり、後から他の属性情報を計測データに付け加えたり、計測データの証明力に関わらない属性情報であってもそれに変更を加えたりすると、計測データ自身が異なるデータとなってしまい、電子署名の検証が不可能になる可能性があった。

【００２９】そこで、以下に説明する第２の実施例は、電子署名を計算した対象を明確にすることで、後から別の属性情報を追加した際にも電子署名の検証を可能にするものである。

【００３０】第２の実施例についてＥｘｉｆ（Ｅｘｃｈａｎｇｅａｂｌｅ　ｉｍａｇｅ　ｆｉｌｅ　ｆｏｒｍａｔ　ｆｏｒ　ｄｉｇｉｔａｌ　ｓｔｉｌｌ　ｃａｍｅｒａ）の画像フォーマットを例にして説明する。図９はＥｘｉｆの画像フォーマットの内容を示す図である。なお、電子署名と、その電子署名の属性情報は、画像撮影条件に関する情報を記述するＥｘｉｆ　ＩＦＤ及びＧＰＳ情報を記述するＧＰＳＩＦＤ、と並列にセキュリティ情報を記述するためのタグの集まりであるＳｅｃｕｒｉｔｙ　ＩＦＤというものを独自に定義し、格納することを実施例として考えている。その際に、Ｅｘｉｆ　ＩＦＤやＧＰＳ　ＩＦＤには計測データ（デジタルカメラの場合にはデジタル写真データ）の証明力を高めるのに役に立つ情報、例えば日付や撮影場所など、計測条件に関わる情報が含まれているため、この情報は改ざんされないよう電子署名により保護したい情報であり、また当然のことながら、計測データ本体そのものと、それを再生するのに必要となる情報についても保護したい対象である。具体的にはＤＱＴマーカからＥＯＩマーカの手前までも保護したいのである。したがって、例えばＥｘｉｆ　ＩＦＤとＧＰＳＩＦＤとＤＱＴマーカからＥＯＩマーカまでについての電子署名であるということを電子署名の属性情報として管理すれば良いことになるが、規格上はＥｘｉｆＩＦＤやＧＰＳ　ＩＦＤの中にはコメントを記録できるようになっており、後からＥｘｉｆ　ＩＦＤの中にコメントを追加してしまった場合、Ｅｘｉｆ　ＩＦＤが以前と異なる状態になってしまうため、電子署名の検証ができなくなってしまう。そこで、電子署名を計算する際に使用したデータを特定する情報を電子署名の属性情報として記録するようにする。

【００３１】次に、撮影されたデジタル画像に対して電子署名を付与する処理手順を図１０に基づいて以下に説明する。ここでは、すでにデジタル画像はＪＰＥＧ（Ｅｘｉｆ）フォーマットに変換されていることを想定している。

【００３２】（１）先ず、保護したい（証拠にしたい）画像データストリーム（例えばＤＱＴマーカからＥＯＩマーカの手前まで）に対して、ＳＨＡ－１やＭＤ５といったハッシュアルゴリズムでハッシュ値（特徴量）を計算する（ステップＳ１００１）。この計算された値をイメージハッシュ値と呼ぶ。

【００３３】（２）イメージハッシュであることを示すタグ番号を用い、Ｖａｌｕｅ部として先のイメージハッシュ値を持つＴＬＶデータエレメント（Ｔａｇ（図中「Ｔ」で表記），Ｌｅｎｇｔｈ（図中「Ｌ」で表記），Ｖａｌｕｅ（図中「Ｖ」で表記））を作成する（ステップＳ１００２）。この作成されたものをイメージハッシュデータエレメントと呼ぶ。

【００３４】（３）Ｅｘｉｆフォーマットに対して新しく独自に定義したＳｅｃｕｒｉｔｙＩＦＤに、先のイメージハッシュデータエレメントを追加する（ステップＳ１００３）。

【００３５】（４）Ｅｘｉｆ　ＩＦＤ、ＧＰＳ　ＩＦＤ、Ｓｅｃｕｒｉｔｙ　ＩＦＤに含まれる、証拠写真として役に立つデータエレメントのタグのリストを作成する（ステップＳ１００４）。これをハッシュタグリストと呼ぶ。なお、このハッシュタグリストにはＥｘｉｆ　ＩＦＤの中の撮影日時データエレメントや、Ｓｅｃｕｒｉｔｙ　ＩＦＤの中のイメージハッシュデータエレメント、撮影者データエレメントなども含まれることになる。

【００３６】（５）ハッシュタグリストに含められたタグに対応する各データエレメントのＶａｌｕｅ部（Ｖａｌｕｅ部が４バイトを超えていて別の場所に本来のＶａｌｕｅ部が記録されている場合には、その別の場所に格納されているＶａｌｕｅ部）を順にＳＨＡ－１やＭＤ５といったハッシュアルゴリズムにかけ、一つのハッシュ値を計算する（ステップＳ１００５）。この計算された値をデータハッシュ値と呼ぶ。

【００３７】（６）データハッシュであることを示すタグ番号を用い、Ｖａｌｕｅ部としてそのデータハッシュ値を持つＴＬＶデータエレメントを作成する（ステップＳ１００６）。この作成されたものをデータハッシュデータエレメントと呼ぶ。

【００３８】（７）先のデータハッシュ値を、デジタルカメラの内部記憶媒体にあるプライベートキーで暗号化する（ステップＳ１００７）。この暗号化されたものをデータ署名と呼ぶ。

【００３９】（８）データ署名であることを示すタグ番号を用い、Ｖａｌｕｅ部としてそのデータ署名の値を持つＴＬＶデータエレメントを作成する（ステップＳ１００８）。この作成されたものをデータ署名データエレメントと呼ぶ。

【００４０】（９）Ｓｅｃｕｒｉｔｙ　ＩＦＤに先のデータハッシュデータエレメントと、データ署名データエレメントを追加する（ステップＳ１００９）。

【００４１】（１０）できあがったＥｘｉｆ画像データをデジタルカメラの大容量記憶媒体に記録する。

【００４２】詳細には述べていないが、ＴＩＦＦのデータ記述方法と同様、ＴＬＶのＶの部分が４バイトを超える場合（ハッシュ値などは８バイト程度）には、Ｖに別の場所を指すオフセットポインタを記録し、その別の場所にＶの値を記録するようにする。

【００４３】このようにして作成された電子署名付きのデジタルカメラの画像は、以下のような処理手順によって、その真正性が検証できる。

【００４４】先ず、ＪＰＥＧ（Ｅｘｉｆ）画像から、データ署名データエレメントのＶａｌｕｅ部を取り出す。データ署名をデジタルカメラのパブリックキーで復号する。ＪＰＥＧ（Ｅｘｉｆ）画像から、データハッシュデータエレメントのＶａｌｕｅ部を取り出す。検証用データハッシュ値とデータハッシュ値が一致するかどうか確認する。一致しなければ、画像データに何かしらの改ざんが行われている。ＪＰＥＧ（Ｅｘｉｆ）画像から、ハッシュタグリストデータエレメントのＶａｌｕｅ部を取り出す。ハッシュタグリストに記録されているタグに該当するデータエレメントのＶａｌｕｅ部を順に取り出し、ハッシュアルゴリズムにかけてハッシュ値を計算する。再計算ハッシュ値と先のハッシュ値が一致するかどうか確認する。一致しなければ、画像データに何かしらの改ざんが行われている。ＪＰＥＧ（Ｅｘｉｆ）画像から、イメージハッシュデータエレメントのＶａｌｕｅ部を取り出す。ＪＰＥＧ（Ｅｘｉｆ）画像から、保護している画像データストリーム部を取り出し、ハッシュアルゴリズム（ＳＨＡ－１やＭＤ５など）にかけてハッシュ値を計算する。検証用イメージハッシュ値とイメージハッシュ値が一致するかどうか確認する。一致しなければ、画像データに何かしらの改ざんが行われている。以上の処理で異常が見つからなければ、画像データは改ざんされていない（改ざんされた可能性は極めて低い）ため、真正性が確保されていると判断できる。

【００４５】このような処理は、電子署名を埋め込む際の処理手順を逆に辿ったようなやり方をしているが、当然のことながら、電子署名を埋め込むのと同じ手順を追ってハッシュ値などを計算し、最後にプライベートキーで暗号化する部分を、逆に画像データに埋め込まれているデータ署名をパブリックキーで復号してデータハッシュ値を比較するという方法をとることもできる。

【００４６】なお、上記実施例ではデジタルカメラを例として説明したがスキャナ等の画像読取手段によって光学的に読み取った画像データあるいはＦＡＸ等で送受信された画像データ等のように画像処理装置によって得られた画像データにも適用できることは言うまでもない。更に、本発明は上記実施例に限定されるものではなく、特許請求の範囲内の記載であれば多種の変形や置換可能であることは言うまでもない。

【００４７】

【発明の効果】以上説明したように、本発明によれば、物理的な計測対象を計測した物理量の計測データを管理するデジタル計測機器において、公開鍵暗号方式の電子署名に用いる少なくとも一対の公開鍵と秘密鍵を鍵生成アルゴリズムによって生成する鍵生成手段を有することに特徴がある。よって、生成した秘密鍵は製造メーカすら知り得ない。

【００４８】また、計測データに対して秘密鍵を用いて計算した電子署名を計測データと共に記録することや秘密鍵により署名された外部から書き替え不可能な公開鍵証明書を記憶することにより、秘密鍵を公開せずとも公

開鍵証明書を作成する際に使用した秘密鍵に対応する公開鍵のみで良い。

【００４９】更に、計測された順番を示す、外部からの書き替え不可能なシーケンス番号を収容し、該シーケンス番号を計測データと共に記録することにより、計測データの前後関係が混乱しないようにすることができる。

【００５０】また、少なくとも１つの外部認証コードを収容し、該外部認証コードに対する外部認証が成立したときに鍵生成アルゴリズム、電子署名及びシーケンス番号の更新を可能とすることにより、計測したデータの証明力を長期間維持できる。

【００５１】更に、画像計測機器により得られた画像に電子署名を埋め込むので画像計測機器で得た画像が改ざんされていないかどうか検証できるようになっている。その際、デジタル画像に電子署名を格納するとデジタル画像そのものが電子署名を格納したことによって変化してしまうことがある。また、後から画像付帯情報を追加することもできなくなる。それを防ぐために、画像のイメージデータストリーム部の特徴量を画像付帯情報として格納し、電子署名を計算する際には、どの画像付帯情報を使用して署名を計算したのかを明確にした。そうすることで電子署名を格納したことによって画像データの、証拠写真と関わらない部分の付帯情報についても変更や追加ができるようになった。

【図面の簡単な説明】

【図１】本発明の第１の実施例に係るデジタル計測機器の構成の概略を示すブロック図である。

【図２】本実施例における計測データに対する処理の流れを示すフローチャートである。

【図３】本実施例における電子署名の格納の様子を示す図である。

【図４】本実施例におけるキーペア生成処理の様子を示す図である。

【図５】本実施例におけるキーペアの生成処理の流れを示すフローチャートである。

【図６】本実施例における外部認証の様子を示す図である。

【図７】本実施例における暗号アルゴリズムの更新処理の様子を示す図である。

【図８】入れ替え可能な暗号処理プロセッサを付加した例の構成を示すブロック図である。

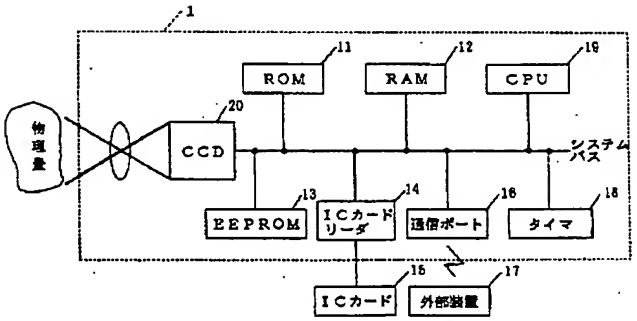
【図９】画像フォーマットの内容を示す図である。

【図１０】本発明の第２の実施例に係る画像計測機器における電子署名の格納処理手順の様子を示す図である。

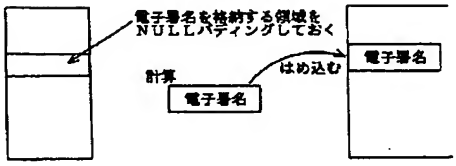
【符号の説明】

１１：ＲＯＭ、１２：ＲＡＭ、１３：ＥＥＰＲＯＭ、１４：ＩＣカードリーダ、　１５：ＩＣカード、１６：通信ポート、１７：外部装置、１８：タイマ、１９：ＣＰＵ、２０：ＣＣＤ、２１：暗号処理プロセッサ。

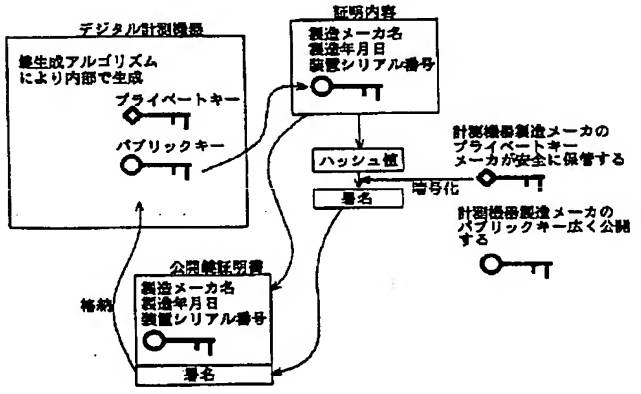
【図１】



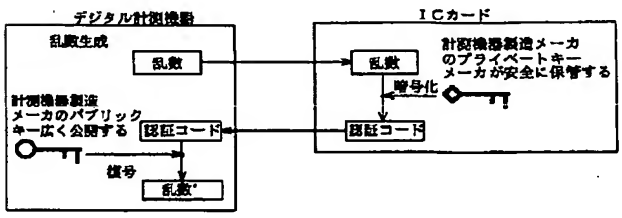
【図３】



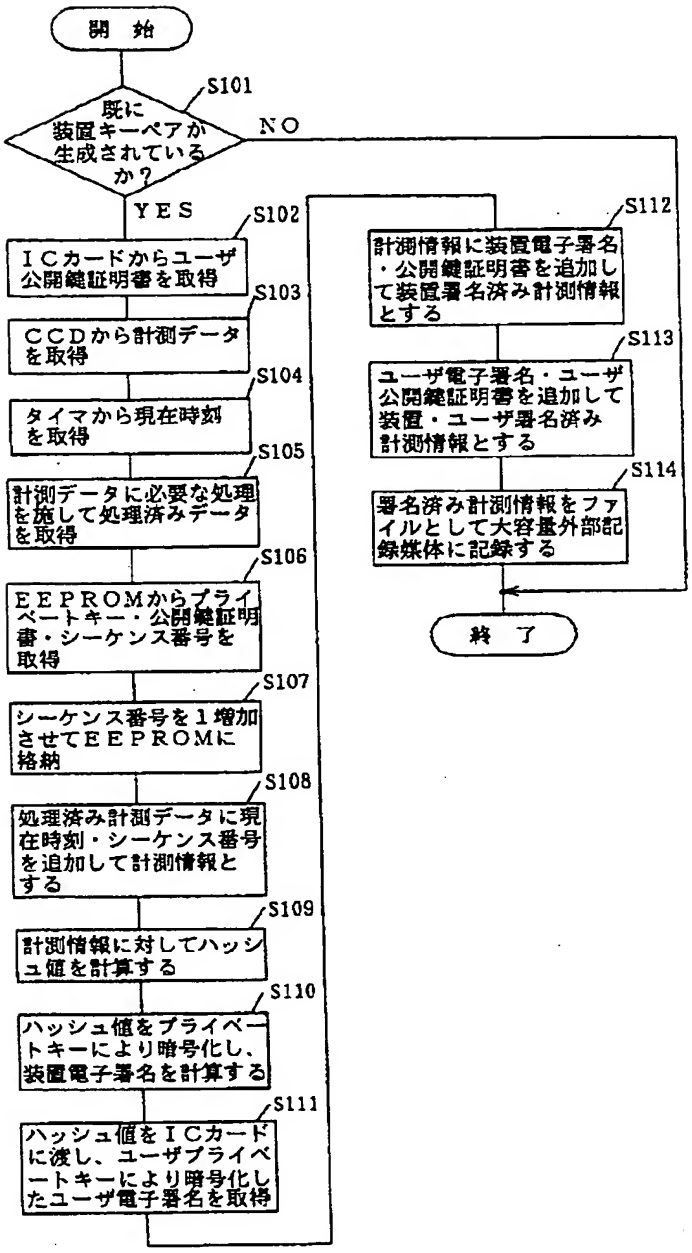
【図４】



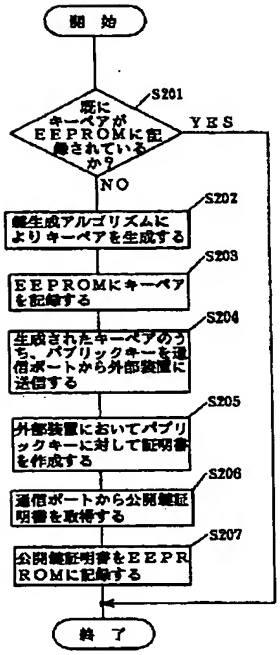
【図６】



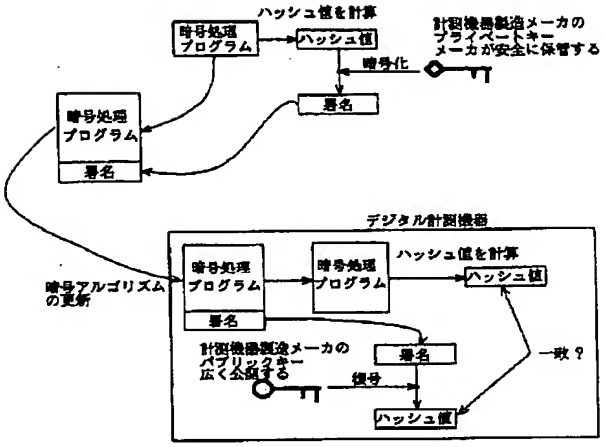
【図２】


開　始
S101
既に装置キーペアが生成されているか？
NO
YES
S102
ＩＣカードからユーザ公開鍵証明書を取得
S103
ＣＣＤから計測データを取得
S104
タイマから現在時刻を取得
S105
計測データに必要な処理を施して処理済みデータを取得
S106
ＥＥＰＲＯＭからプライベートキー・公開鍵証明書・シーケンス番号を取得
S107
シーケンス番号を１増加させてＥＥＰＲＯＭに格納
S108
処理済み計測データに現在時刻・シーケンス番号を追加して計測情報とする
S109
計測情報に対してハッシュ値を計算する
S110
ハッシュ値をプライベートキーにより暗号化し、装置電子署名を計算する
S111
ハッシュ値をＩＣカードに渡し、ユーザプライベートキーにより暗号化したユーザ電子署名を取得
S112
計測情報に装置電子署名・公開鍵証明書を追加して装置署名済み計測情報とする
S113
ユーザ電子署名・ユーザ公開鍵証明書を追加して装置・ユーザ署名済み計測情報とする
S114
署名済み計測情報をファイルとして大容量外部記録媒体に記録する
終　了

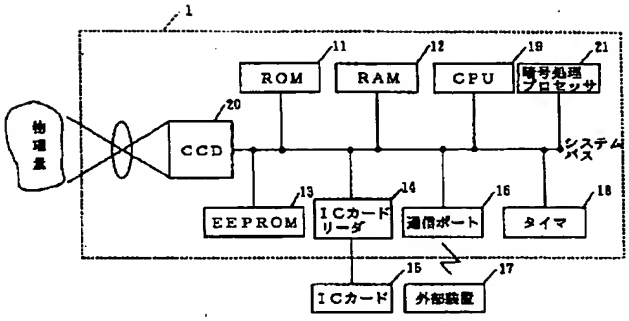
【図５】


開　始
S201
既にキーペアがＥＥＰＲＯＭに記録されているか？
YES
NO
S202
鍵生成アルゴリズムによりキーペアを生成する
S203
ＥＥＰＲＯＭにキーペアを記録する
S204
生成されたキーペアのうち、パブリックキーを通信ポートから外部装置に送信する
S205
外部装置においてパブリックキーに対して証明書を作成する
S206
通信ポートから公開鍵証明書を取得する
S207
公開鍵証明書をＥＥＰＲＯＭに記録する
終　了

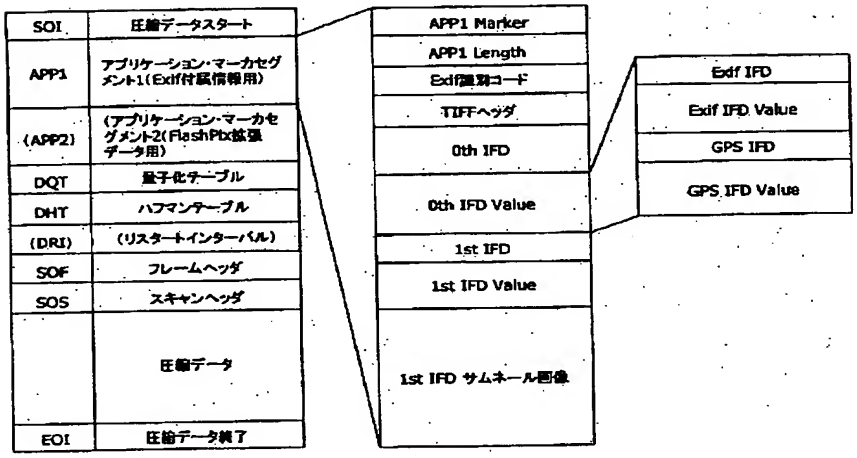
【図７】


ハッシュ値を計算
暗号処理プログラム
ハッシュ値
暗号化
計測機器製造メーカのプライベートキーメーカが安全に保管する
署名
暗号処理プログラム
署名
デジタル計測機器
暗号処理プログラム
暗号処理プログラム
ハッシュ値を計算
ハッシュ値
暗号アルゴリズムの更新
署名
計測機器製造メーカのパブリックキー広く公開する
署名
一致？
復号
ハッシュ値

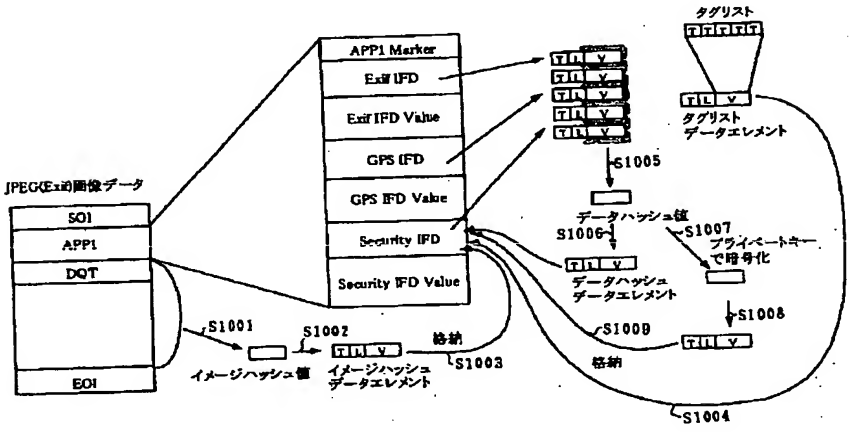
【図８】


1
ROM
11
RAM
12
CPU
19
暗号処理プロセッサ
21
物理量
CCD
20
システムバス
EEPROM
13
ICカードリーダ
14
通信ポート
16
タイマ
18
ICカード
15
外部装置
17

【図９】


SOI
圧縮データスタート
APP1
アプリケーション・マーカセグメント1(Exif付属情報用)
(APP2)
(アプリケーション・マーカセグメント2(FlashPix拡張データ用)
DQT
量子化テーブル
DHT
ハフマンテーブル
(DRI)
(リスタートインターバル)
SOF
フレームヘッダ
SOS
スキャンヘッダ
圧縮データ
EOI
圧縮データ終了
APP1 Marker
APP1 Length
Exif識別コード
TIFFヘッダ
0th IFD
0th IFD Value
1st IFD
1st IFD Value
1st IFD サムネール画像
Exif IFD
Exif IFD Value
GPS IFD
GPS IFD Value

【図１０】


JPEG(Exif)画像データ
SOI
APP1
DQT
EOI
APP1 Marker
Exif IFD
Exif IFD Value
GPS IFD
GPS IFD Value
Security IFD
Security IFD Value
タグリスト
タグリストデータエレメント
S1005
データハッシュ値
S1006
S1007
プライベートキーで暗号化
データハッシュデータエレメント
S1008
S1009
格納
S1001
S1002
格納
S1003
イメージハッシュ値
イメージハッシュデータエレメント
S1004

フロントページの続き

(51)Int.Cl.[7]	識別記号	F I		テーマコード（参考）
		Ｈ０４Ｌ　9/00	６０１Ｆ	

Japanese Publication number : 2000-215379 A

CLAIMS

[Claim(s)]
[Claim 1] The digital measuring machine machine which measures the physical candidate for measurement and is characterized by having a key generation means used for the electronic signature of a public key cryptosystem to generate the public key and private key of a pair with a key generation algorithm at least, in the digital measuring machine machine which gives the electronic signature of a public key cryptosystem to the measurement data of the measured physical quantity, and manages measurement data.
[Claim 2] The digital measuring machine machine according to claim 1 which records the electronic signature calculated using said private key to said measurement data with said measurement data.
[Claim 3] The digital measuring machine machine according to claim 1 which memorizes the public key certificate which was signed with said private key, and which is not rewritable from the exterior.
[Claim 4] The digital measuring machine machine according to claim 1 which holds the sequence number which shows the measured sequence, and which is not rewritable from the exterior, and records this sequence number with said measurement data.
[Claim 5] The digital measuring machine machine according to claim 1 to 4 which enables renewal of said key generation algorithm, said electronic signature, and said sequence number when at least one external authorization code is held and the external authentication over this external authorization code is materialized.
[Claim 6] The image measuring machine machine which has the characteristic quantity of an image as a part of image incidental information on an image data format, and is characterized by calculating electronic signature and storing in an image data format by making the calculated electronic signature into image incidental information from image incidental information using the private key of an image measuring machine machine in the image measuring machine machine which gives the electronic signature of a public key cryptosystem to image data.
[Claim 7] The image measuring machine machine according to claim 6 stored in the image data format by making into image incidental information whether to have used one information of the image incidental information when calculating electronic signature.
[Claim 8] The image measuring machine machine according to claim 6 which uses the private key of an image measuring machine machine based on characteristic quantity, and

is stored in an image data format by making into image incidental information the electronic signature which calculated and calculated electronic signature while storing the characteristic quantity which calculated characteristic quantity and was calculated as image incidental information about the image incidental information containing the characteristic quantity of an image.

[Claim 9] While storing the characteristic quantity which calculated characteristic quantity and was calculated as image incidental information about the image incidental information containing the characteristic quantity of an image Use the private key of an image measuring machine machine based on characteristic quantity, and it stores in an image data format by making into image incidental information the electronic signature which calculated and calculated electronic signature. Moreover, the image measuring machine machine according to claim 6 which calculates electronic signature using the private key stored in the enternal memory means with which the image measuring machine machine was equipped based on characteristic quantity, and also stores the electronic signature concerned in an image data format as image incidental information.

[Claim 10] The image incidental information used in case the characteristic quantity used for count of electronic signature is calculated is an image measuring machine machine containing the serial number of image data according to claim 6 to 9.

[Claim 11] The image incidental information used in case the characteristic quantity used for count of electronic signature is calculated is an image measuring machine machine containing the serial number of an image measuring machine machine according to claim 6 to 9.

[Claim 12] The image incidental information used in case the characteristic quantity used for count of electronic signature is calculated is an image measuring machine machine containing the public key used as the pair of the private key used for count of electronic signature according to claim 6 to 9.

[Claim 13] The image incidental information used in case the characteristic quantity used for count of electronic signature is calculated is an image measuring machine machine according to claim 6 to 9 which contains the public key used as the pair of the private key used for count of electronic signature in the form of a public key certificate.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention changes into digital data the input obtained from a digital camera, a scanner, a sensor, FAX (modem), etc. by the detail about a digital measuring machine machine and an image measuring machine machine, and relates to the data security of the equipment which processes management, transmission, etc. to the digital data.

[0002]

[Description of the Prior Art] Various techniques are developed, in order for informational electronization to progress quickly, to exchange all information mutually through a network or portable media as electronic data and to secure the security of the electronic data in recent years. the security technique of the electronic data currently generally examined -- mainly -- the contents of data, such as a secrecy technique of data, an alteration detection technique of data, and a management (authentication is included) technique of the access privilege to data, -- not paying one's attention -- an edge -- while there were many security techniques treated as a lump, the ED to which the contents of the electronic data are related for whether being the right or not from the first was seldom made. However, if the data from the first which are going to secure security are inaccurate, no semantics will be made even if it secures the security of the data. if data from the first are electronically generated by artificial actuation from the beginning -- the contents of the data -- the right -- the implementer who created the data like a Prior art in order to have guaranteed things, or its data -- being related -- responsibility -- **** -- adding the electronic signature of those who are etc. will be processed.

[0003] Then, the method of storing the private key of the digital camera proper in a digital camera, calculating electronic signature on U.S. Pat. No. 5,499,294 specifications, as a conventional example, using the private key concerned to the image file photoed with the digital camera, and recording on a medium with an image file is indicated. The private key stored in a detail at the digital camera is Secure in a digital camera. It can ROM-ize to Processor, can be recorded on it, and can read no longer from the exterior. Moreover, the public key corresponding to the private key is stamped on the body of a digital camera. Furthermore, the parameter which shows the public key and photography situation is printed to the periphery of the image photoed with the digital camera, and it is made to perform electronic signature to it to the whole image. Therefore, as for the image photoed with the digital camera, the certification force is heightened. In addition, the public key corresponding to a digital camera is premised on the manufacture manufacturer of a digital camera opening to the public widely.

[0004]

[Problem(s) to be Solved by the Invention] However, according to the above-mentioned conventional example, those correlation may not be clear anymore when an image file is moved to a personal computer etc., since the photoed image file and the electronic signature file which the digital camera calculated to it are separate. Therefore, it was not clear anymore which in spite of having performed processing which heightens the certification force of an image file with much trouble, is an electronic signature file, and there was a problem of it becoming impossible to verify the bona fides of an image file after all.

[0005] Moreover, although the manufacture manufacturer of a digital camera generates the pair of a private key and a public key and he is trying to record on the interior of a camera, that the digital camera manufacture manufacturer knows the private key also had the problem that it was connected with reducing the certification force.

[0006] Furthermore, although it was preventing from changing after setting up a setup of a timer with a built-in digital camera at the manufacture time, it was what may naturally happen that a timer goes wrong gradually, and it was a problem that it cannot be reset as right time of day. It was a problem that record of the time of day itself becomes impossible to it when the lithium ion battery which is the power source of a timer goes out to it.

[0007] Moreover, although manufacture meter is to exhibit widely all the public keys assigned to digital camera each in the above-mentioned conventional example, having considered the case where many digital cameras were manufactured very much, that only the part of the number exhibits a public key had the problem that the public key which complicatedness increases and corresponds out of a vast quantity of public key lists in the case of bona-fides verification of an image had to be discovered.

[0008] Furthermore, since the digital instrument for general users like a digital camera was assumed, there were whose having recorded the data etc. and a problem that it was not taken into consideration at all about ********. For example, it is because it may become important who measured the data especially in the case of medical-application metering devices, such as a CT scanner and digital endoscope equipment, (photography).

[0009] moreover -- it not being taken into consideration about an addition and exchange of the electronic signature algorithm inside equipment, or renewal of a key, but carrying a new algorithm in a new product model, since the short digital instrument of the comparatively cheap life cycle for general users like a digital camera is assumed -- **** -- it is not stated. However, in the case of large sum digital medical equipment like a CT scanner, the life cycle also had the problem that it might be said that it will be long and the reinforcement of cryptographic algorithm will become weak relatively in an engine shorter than the life of equipment, for example.

[0010] This invention aims at offering the digital measuring machine machine and image measuring machine machine for solving these troubles which it is [machine] and have the dependability and the certification force of the contents of electronic digital data heightened.

[0011]

[Means for Solving the Problem] This invention has the description in having a key generation means used for the electronic signature of a public key cryptosystem to generate the public key and private key of a pair with a key generation algorithm at least in the digital measuring machine machine which manages the measurement data of the physical quantity which measured the physical candidate for measurement, in order to solve said trouble. Therefore, even a manufacture manufacturer cannot know the generated private key.

[0012] Moreover, it is good only at the public key corresponding to the private key used when a private key was not exhibited but ** also drew up a public key certificate by memorizing the public key certificate which cannot rewrite the electronic signature calculated using the private key to measurement data from the exterior signed with recording with measurement data, or a private key.

[0013] Furthermore, the context of measurement data can be prevented from getting confused by holding the sequence number which shows the measured sequence and which is not rewritable from the exterior, and recording this sequence number with measurement data.

[0014] Moreover, when at least one external authorization code is held and the external authentication over this external authorization code is materialized, the certification force of the measured data can be maintained for a long period of time by enabling renewal of a key generation algorithm, electronic signature, and a sequence number.

[0015] Furthermore, it has the characteristic quantity of an image as a part of incidental information on an image data format as another invention. By calculating electronic signature using the private key of an image measuring machine machine from image incidental information, and carrying out additional storing into an image data format as image incidental information Since electronic signature is embedded in the image obtained from the image measuring machine machine, can verify whether the image photoed with the image measuring machine vessel is altered, and In case the characteristic quantity of an image is stored as image incidental information and electronic signature is calculated, it can carry out clear [of using which image incidental information the signature was calculated]. It came to be able to perform modification and an addition by having stored electronic signature by doing so also about the incidental information on the part without regards to the documentary photography of image data.

[0016]

[Embodiment of the Invention] It has a key generation means used for the electronic signature of a public key cryptosystem to generate the public key and private key of a pair with a key generation algorithm at least.

[0017]

[Example] Hereafter, the example of this invention is explained based on a drawing. First, with the contents of electronic data, especially the measurement data of physical quantity, if an example is given, the reconstruction image data measured and calculated with CT (Computed Tomography) equipment used by the image data photoed with the digital camera or medicine will be mentioned. Electronic data (when crossing the data to others or showing it, it is thought that it will be necessary to guarantee) which will need to guarantee the measured physical quantity and correlation, such as data after performing processings (the case of a digital camera the case of a CT scanner FBP (Filtered Back Projection) image-reconstruction processings by law, such as compression processing of an image and gradation transform processing etc.) peculiar to the metering device from the measured data like these data, is applicable. And even if it is equipments which generally are not called a metering device, such as a digital camera and a CT scanner, it is called the "digital measuring machine machine" from the above backgrounds.

[0018] Drawing 1 is a block which shows the configuration of the digital measuring machine machine concerning the 1st example of this invention. In addition, it shall be explained below as a digital measuring machine machine of this example, using a digital

camera as an example. This example shown in this drawing is the cryptographic algorithms for electronic signature (for example, RSA, MD5, etc.), and cryptographic algorithm (for example, DES (Date Encryption Standard).) used for external authentication. Although this DES is the cryptographic algorithm of a private key cryptosystem, as long as it is applicable to external authentication, the cryptographic algorithm of what kind of method is sufficient as it. ROM11 which stores an image data compression algorithm (for example, JPRG), a random-number-generation algorithm, and the Maine control program, RAM12 to which the Maine control program, various algorithms, a private key, a sequence number, an external authentication key, etc. are loaded if needed, EEPROM13 which stores the private key used for the electronic signature of a public key cryptosystem, a public key certificate (an authentication engine's signature and public key), and a sequence number and an external authentication key, Record the digital image information which added a sequence number, time of day, electronic signature, etc. to the photoed digital photography image data. For example, the communication link port 16 for performing the exchange by the communication link with the IC card reader 14 and external device 17 which perform read-out/writing for the information concerned on IC cards 15, such as a memory card, It is constituted including CPU19 which performs the timer 18 which acquires time-of-day data, and various kinds of operations, and controls each component, and CCD20 which changes the photoed image into electronic data.

[0019] Next, if actuation of this example is explained and a shutter carbon button will be pushed, CPU19 acquires photography image data from CCD20, and stores it in RAM12 at the same time it acquires time-of-day data from a timer 18 and memorizes it to RAM12. And the stored image data is compressed. Moreover, the sequence number added to the sequence number one is stored in EEPROM13 at the same time it takes out a sequence number from EEPROM13. The sequence number previously taken out at the head of the compressed image data and the time-of-day data acquired from the timer 18 are added. And the electronic signature is added to previous image information to the done image information, and it stores in IC card 15 as photography information as one lump. In case a private key, a public key certificate, a sequence number, and a time-of-day setup are changed, if the case where DES is used for the algorithm used for external authentication is taken for an example, the following procedures will perform external authentication processing which should be performed beforehand.

[0020] First, a random number is generated inside and the random number is sent out to an external device. It compares with the code which enciphered the authorization code with reception from the external device, and enciphered the random number generated previously with the external authentication key. It supposes that external authentication was materialized when those codes were in agreement, and is the security status (flag which has managed this by RAM.). an initial state -- FALSE -- carrying out -- it changes into TRUE. With reference to the security status first managed inside when modification of a private key, a public key certificate, a sequence number, and a time-of-day setup is

required from the exterior, when it serves as FALSE, a demand is not received. On the other hand, when it is TURE, a demand is received, and processing according to the demand is performed. Processing changes the security status into FALSE.

[0021] Next, it explains below that processing flows to the measurement data in this example. First, it investigates whether the key pair (this key pair is a pair of a private key and a public key) of equipment is already generated (step S101), when not carried out, processing is ended, but if generated, a user public key certificate will be acquired from IC card 15 of drawing 1 (step S102). Measurement data (photography data) are acquired from CCD20, and current time is further acquired from a timer 18 (steps S103 and S104). And conversion to processing required for the acquired measurement data, for example, compression, CT image reconstruction, and a standard data format etc. is performed, and measurement data [finishing / processing] are acquired (step S105). Next, a private key, a public key certificate, and a sequence number are acquired from EEPROM13 (step S106). One **** is made the acquired sequence number and it stores in EEPROM13 (step S107). Let the thing which was having current time and a sequence number added to measurement data [finishing / processing] be measurement information (step S108). A hash value is calculated to this measurement information (step S109). It is enciphered by the private key and the calculated hash value calculates the electronic signature of equipment (step S110). The user electronic signature which enciphered the hash value by which count was carried out [above-mentioned] by the private key of delivery and a user to the IC card is acquired (step S111). And the electronic signature and public key certificate of equipment are added to measurement information, and it considers as measurement information [finishing / the signature of equipment] (step S112). Furthermore, user electronic signature and a user public key certificate are added, and it considers as the signed measurement information of equipment and a user (step S113). It records on a mass external record medium by considering done signed measurement information as a file (step S114 (or it sends out to an external device from the communication link port 16)).

[0022] Thus, a signature of a user is generated using enternal memory means, such as an IC card with a code processing facility and a memory storage function, and the metering device itself is not attesting the user only by having given the signed measurement information on equipment with a user's public key certificate. If signed measurement information is verified, although the user would be whom or this will carry out "later" authentication, since it is made, there is. On the other hand, as long as the metering device itself can attest a user beforehand, you may be other approaches, a user is attested for a metering device, as long as it is clear and is, a user name may only be given to processed measurement data with a sequence number etc., and electronic signature processing may be performed. When not using an IC card, a metering device does not need to carry the IC card reader 14. It assumes that the serial number of equipment, the manufacture meter name, etc. are indicated by the public key certificate of equipment, and the user name which can specify a user as a user's public key certificate, affiliation, etc. are indicated.

About the public key certificate of equipment, equipment is enabled to send out outside according to the demand from the outside. Moreover, in this example, although electronic signature is immediately created after creating measurement information, since computation time starts creation of electronic signature, un-arranging may arise to measure continuously. Then, the created measurement information is recorded on mass external storage as it is, and before sending out outside later, or before it removes a mass storage medium from measurement information, you may make it create and give electronic signature. In that case, it is necessary to prevent from accessing the measurement information which has not given electronic signature -- mass external storage prevents from removing from the body of a metering device etc. -- from an external device until it gives electronic signature.

[0023] Moreover, although he is trying to only add incidental information (current time, a sequence number, public key certificate, etc.) behind processed measurement data, since the data of arbitration can be embedded as an image data format, for example in the case of a JPEG image, these incidental information is also recordable on the part using it. By doing so, though it is the file where electronic signature was embedded, it also becomes possible for the existing image display program etc. to process. Since that it must be careful in that case has the absolute location for where image data has begun from as a tag in the case of TIFF etc., when electronic signature is embedded, the absolute location will shift. Then, in order to avoid such a problem, as shown in drawing 3 , only the part which embeds electronic signature beforehand secures a field, and the field is fill uped with the value decided beforehand, calculates a hash value to the whole data on it, and generates electronic signature. And it is also possible to embed the generated electronic signature to the field secured beforehand. Before performing data measurement, key pair generation processing must be performed beforehand. For example, a metering-device manufacture manufacturer performs this processing before shipment at works.

[0024] Next, it investigates whether the key pair is already recorded on EEPROM of a measuring machine machine (step S201), and if key pair generation processing is explained based on drawing 4 and drawing 5 , since it is not necessary to generate if the key pair is recorded, processing will be ended. On the other hand, if the key pair is not recorded, as shown in drawing 4 , a key generation algorithm will generate a key pair (step S202). And the generated key pair is recorded on EEPROM (step S203). Next, a public key is transmitted to an external device through a communication link port among key pairs (step S204). As shown in drawing 4 , in an external device, a public key certificate is drawn up to a public key, and the public key certificate concerned is passed to a digital measuring machine machine through a communication link port (steps S205 and S206). And a public key certificate is recorded on EEPROM (step S207).

[0025] Moreover, if the processing which sets up the internal timer of a metering device is said in an easy example, a keypad will be attached in a metering device, a password is entered from a keypad, and if a metering device collates with the password currently held inside and is right, how to permit setting modification of a timer can be considered. Since

the metering device carries IC card reader like above-mentioned this example in others, it is also thought of that a specific IC card enables it to change a setup of a timer only into an insertion ********** case. In order for being inserted to verify whether it is a specific IC card, the following approaches can be taken, for example. As shown in drawing 6 , a measuring machine machine manufacturer's public key is beforehand stored in the interior of a metering device. And if the random number which the metering device generated first, and random-number [which decoded the authorization code from an IC card]' are in agreement, the IC card will have a secret key and it can attest that it is a specific code.

[0026] About an update process of cryptographic algorithm, if setting processing of a timer explains, for example, what enables it to receive a new code processing program through a communication link port only to the midst which is inserting the specific IC card can be considered. Or if a manufacture manufacturer's electronic signature is given to a code processing program and a metering device is passed as shown in drawing 7 , how to use [for a metering device to verify the electronic signature, to store the code processing program in an internal-storage medium, if it is verifiable that it is right electronic signature, and] it for cipher processing will also be considered. Also in this example, it assumes having held a manufacture manufacturer's public key beforehand to the metering device. It assumes that the algorithm which calculates a hash value, the algorithm which generates a key pair, and the algorithm to encipher and the algorithm to decode are contained in a code processing program.

[0027] Moreover, although stated as an update process of cryptographic algorithm above, it does not update about cryptographic algorithm but only an addition may not be made to be not possible. Although what has reinforcement high with the cryptographic algorithm registered later being natural should be used, when an old code processing program is brought and someone installs in a metering device unjustly, it can prevent the certification force of a metering device in which the newest code processing program is already carried declining. It does not come out so much and possibility that a defect will be found in the newest cryptographic algorithm is large compared with an old algorithm. Therefore, you may make it give both the electronic signature of an old algorithm, and the electronic signature by the newly installed cryptographic algorithm to measurement information. Moreover, about cryptographic algorithm, since a new algorithm has large possibility of needing computational complexity more, it may be made to replace the processor which performs not exchange but the code processing program as a code processing program. In that case, although a cipher-processing processor needs to attest whether it is what was made by the just manufacture manufacturer, the structure can apply the completely same processing as the processing which verifies previously whether it is a specific IC card. A cipher-processing processor module can consider the gestalt of a PCMCIA card etc. Or the physical interface between a cipher-processing processor and a metering device may be made special, or approaches, such as making special the protocol between the processor of a metering device and a cipher-processing processor, and making it secret, may be taken. In such a case, it is not necessary to attest a cipher-processing processor. Detailed

explanation is omitted although the configuration of the metering device at the time of dividing into the processor of a metering device and the processor for cipher processing becomes like drawing 8 .

[0028] In the 1st example of the above, the field which stores electronic signature in measurement data was reserved, the digital measuring machine machine calculated electronic signature to the whole measurement data in the condition of having carried out NULL padding of the part beforehand, and the approach of storing the electronic signature in the previous reservation field was taken. There was a problem to come to store other information, for example, a comment etc., in measurement data further, after storing electronic signature in measurement data in the case of this approach. That is, even if it was the attribute information without regards to the certification force of measurement data, when it added other attribute information to measurement data later, or modification was added to it, it may have become data with which the measurement data itself differ, and verification of electronic signature may have become impossible.

[0029] Then, the 2nd example explained below is clarifying the object which calculated electronic signature, and also when it adds another attribute information later, it enables verification of electronic signature.

[0030] About the 2nd example, the graphics format of Exif (Exchangeable image file format for digital still camera) is made into an example, and is explained. Drawing 9 is drawing showing the contents of the graphics format of Exif. In addition, the attribute information on electronic signature and its electronic signature is Exif which describes the information about image photography conditions. Security which is the assembly of the tag for describing security information to GPSIFD and juxtaposition which describe IFD and GPS information It considers defining a thing called IFD uniquely and storing it as an example. In that case, it is Exif. IFD and GPS Information which is helpful for raising the certification force of measurement data (the case of a digital camera digital photography data) to IFD, For example, since the information in connection with measurement conditions, such as the date and a photography location, is included, This information is information to protect by electronic signature so that it may not be altered, and it is an object to protect also about the information which is needed for reproducing it with the body of measurement data itself with a natural thing. I want to specifically protect to a DQT marker to an EOI marker's this side. Therefore, Exif Although what is necessary will be just to manage that it is the electronic signature attached even to an EOI marker from IFD, GPSIFD, and a DQT marker as attribute information on electronic signature A specification top is ExifIFD and GPS. A comment can be recorded now into IFD. From after to Exif It is Exif when the comment has been added into IFD. Since IFD will be in the condition of differing from before, verification of electronic signature will become impossible. Then, the information which specifies the data used when calculating electronic signature is recorded as attribute information on electronic signature.

[0031] Next, the procedure which gives electronic signature to the photoed digital image is explained below based on drawing 10 . Here, it has already assumed that the digital image

is changed into the JPEG (Exif) format.

[0032] (1) Calculate a hash value (characteristic quantity) by hash algorithms, such as SHA-1 and MD5, to an image data stream (I want to make it proof) to protect first (step S1001). (to for example, a DQT marker to an EOI marker's this side) This calculated value is called an image hash value.

[0033] (2) Create the TLV data element (Tag (it writes by "T] among drawing), Length (it writes by "L" among drawing), Value (it writes by "V" among drawing)) which has a previous image hash value as a Value section using the tag number which shows that it is an image hash (step S1002). This created thing is called an image hash data element.

[0034] (3) Add a previous image hash data element to SecurityIFD newly defined uniquely to the Exif format (step S1003).

[0035] (4) Exif IFD, GPS IFD, Security The list of tags of the data element which is helpful as documentary photography included in IFD is created (step S1004). This is called a hash tag list. In addition, in this hash tag list, it is Exif. The photography time data element in IFD, and Security The image hash data element in IFD, a photography person data element, etc. will be contained.

[0036] (5) Calculate one hash value by applying the Value section (the Value section stored in the somewhere else when the Value section is over 4 bytes and the original Value section is recorded on somewhere else) of each data element corresponding to the tag included in the hash tag list to order at hash algorithms, such as SHA-1 and MD5, (step S1005). This calculated value is called a data hash value.

[0037] (6) Create the TLV data element which has the data hash value as a Value section using the tag number which shows that it is a data hash (step S1006). This created thing is called a data hash data element.

[0038] (7) Encipher a previous data hash value by the private key in the internal-storage medium of a digital camera (step S1007). This enciphered thing is called a data signature.

[0039] (8) Create the TLV data element which has the value of the data signature as a Value section using the tag number which shows that it is a data signature (step S1008). This created thing is called a data signature data element.

[0040] (9) Security A previous data hash data element and a previous data signature data element are added to IFD (step S1009).

[0041] (10) The done Exif image data is recorded on the mass storage medium of a digital camera.

[0042] Like the data description approach of TIFF, although not stated to a detail, when the part of V of TLV exceeds 4 bytes (a hash value etc. is about 8 bytes), the offset pointer which points somewhere else out to V is recorded, and the value of V is recorded on the somewhere else.

[0043] Thus, the image of the created digital camera with electronic signature can verify the bona fides with the following procedure.

[0044] First, the Value section of a data signature data element is taken out from a JPEG (Exif) image. A data signature is decoded by the public key of a digital camera. The Value

section of a data hash data element is taken out from a JPEG (Exif) image. It checks whether the data hash value for verification and a data hash value are in agreement. if not in agreement -- image data -- what -- it is -- the alteration is performed. The Value section of a hash tag list data element is taken out from a JPEG (Exif) image. A hash value is calculated by taking out in order the Value section of the data element applicable to the tag currently recorded on the hash tag list, and applying to a hash algorithm. It checks whether a re-calculation hash value and a previous hash value are in agreement. if not in agreement -- image data -- what -- it is -- the alteration is performed. The Value section of an image hash data element is taken out from a JPEG (Exif) image. A hash value is calculated by taking out the protected image data stream section from a JPEG (Exif) image, and applying to hash algorithms (SHA-1, MD5, etc.). It checks whether the image hash value for verification and an image hash value are in agreement. if not in agreement -- image data -- what -- it is -- the alteration is performed. If abnormalities are not found in the above processing, since image data is not altered (possibility of having been altered is very low), it can be judged that bona fides are secured.

[0045] Such processing can also take the approach of decoding the data signature currently conversely embedded at image data in the part which calculates a hash value etc. later on and finally enciphers the same procedure as embedding electronic signature with a natural thing although the way of having followed conversely the procedure at the time of embedding electronic signature is carried out by the private key by the public key, and comparing a data hash value.

[0046] In addition, although the above-mentioned example explained the digital camera as an example, it cannot be overemphasized that it is applicable also to the image data obtained with the image processing system like the image data transmitted and received by image data or FAX optically read with image reading means, such as a scanner. Furthermore, this invention is not limited to the above-mentioned example, and if it is the publication in a patent claim, neither deformation of a variety nor a replaceable thing can be overemphasized.

[0047]

[Effect of the Invention] As explained above, according to this invention, the description is in the digital measuring machine machine which manages the measurement data of the physical quantity which measured the physical candidate for measurement to have a key generation means used for the electronic signature of a public key cryptosystem to generate the public key and private key of a pair with a key generation algorithm at least. Therefore, even a manufacture manufacturer cannot know the generated private key.

[0048] Moreover, it is good only at the public key corresponding to the private key used when a private key was not exhibited but ** also drew up a public key certificate by memorizing the public key certificate which cannot rewrite the electronic signature calculated using the private key to measurement data from the exterior signed with recording with measurement data, or a private key.

[0049] Furthermore, the context of measurement data can be prevented from getting

confused by holding the sequence number which shows the measured sequence and which is not rewritable from the exterior, and recording this sequence number with measurement data.

[0050] Moreover, when at least one external authorization code is held and the external authentication over this external authorization code is materialized, the certification force of the measured data can be maintained for a long period of time by enabling renewal of a key generation algorithm, electronic signature, and a sequence number.

[0051] Furthermore, since electronic signature is embedded in the image obtained with the image measuring machine vessel, it can verify whether the image obtained with the image measuring machine vessel is altered. In that case, when electronic signature is stored in a digital image, and the digital image itself stored electronic signature, it may change. It also becomes impossible moreover, to add image incidental information afterwards. In order to prevent it, when the characteristic quantity of the image-data stream section of an image was stored as image incidental information and electronic signature was calculated, it clarified using which image incidental information the signature was calculated. It came to be able to perform modification and an addition by having stored electronic signature by doing so also about the incidental information on the part without regards to the documentary photography of image data.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the outline of the configuration of the digital measuring machine machine concerning the 1st example of this invention.

[Drawing 2] It is the flow chart which shows the flow of the processing to the measurement data in this example.

[Drawing 3] It is drawing showing the situation of storing of the electronic signature in this example.

[Drawing 4] It is drawing showing the situation of the key pair generation processing in this example.

[Drawing 5] It is the flow chart which shows the flow of generation processing of the key pair in this example.

[Drawing 6] It is drawing showing the situation of the external authentication in this example.

[Drawing 7] It is drawing showing the situation of an update process of the cryptographic algorithm in this example.

[Drawing 8] It is the block diagram showing the configuration of the example which added the cipher-processing processor which can be replaced.

[Drawing 9] It is drawing showing the contents of the graphics format.

[Drawing 10] It is drawing showing the situation of the storing procedure of the electronic signature in the image measuring machine machine concerning the 2nd example of this

invention.

[Description of Notations]

11: ROM, 12:RAM, 13:EEPROM, 14:IC card reader 15: An IC card, 16:communication link port, 17:external device, 18:timer, 19:CPU, 20:CCD, 21:cipher-processing processor.